Mobile Device Policy

Introduction

The Mobile Device Policy is one of several Sysco Information Security policies, which support the overarching goal of Information Security to protect the confidentiality, integrity and availability of Sysco business and assets.

- Information accessed via mobile devices, such as internal documents, email, calendars, and contacts, has a significant effect on Sysco business, customers, partners, associates, and investors.
- Lost, stolen, or otherwise compromised mobile devices affect productivity, result in the loss of proprietary Sysco information, and potentially expose Sysco to legal action.

Purpose

The purpose of this policy is to establish rules and communicate the risks of using mobile devices to access Sysco business information, in addition to the following:

- Prevent the mishandling of Sysco information that is accessible via mobile devices
- Ensure the availability and integrity of Sysco information and computing resources
- Prevent negative impact to Sysco brand integrity
- Inform Sysco associates, contractors, and partners of their responsibility to ensure and promote compliance

Scope

This policy applies to the use of any mobile device accessing Sysco network and information facilities; including both company issued and personally owned devices.

This Mobile Device Policy is a Corporate Policy and applies to all Sysco associates, associates of any Sysco subsidiary, and third parties performing services on Sysco's behalf (hereinafter collectively referred to as "You"). For associates, compliance with this Policy is an expectation of employment. For third parties who perform services on Sysco's behalf, compliance with this Policy is a condition of access to Sysco facilities and resources, and of being permitted to perform services for Sysco.

Note: Non-exempt associates are not authorized to configure their mobile devices to automatically receive Sysco information (including email), and must not use mobile devices to distribute Sysco information.

Policy Requirements

- Connecting your Sysco or non-Sysco issued device to the Sysco network (includes configuring a mobile device to receive Sysco email) requires that you understand the risks, and that you agree to the terms outlined in this policy.
- Sysco reserves the right to erase *all content* of any mobile device that accessed the Sysco network, including personal content and removable media.
- Mobile devices that are not on the list of Sysco Corporate Approved Devices are prohibited from connecting to the Sysco network.
- If you disagree with or do not comply with any elements of this policy, your mobile device is not authorized for connection to the Sysco network. If you access the Sysco network but do not comply with this policy, such access is unauthorized.

1. Compromised or Lost Devices

It is your responsibility to initiate the remote deletion of all files from a lost or stolen mobile device within 24 hours of the device being lost or stolen.

- Report the device as lost or stolen to Sysco Customer Support, and the support team will initiate file deletion from the mobile device on your behalf.

2. Secure Mobile Device Configuration

Software will be installed on all mobile devices used to connect to the Sysco network, so the devices will be automatically updated to align with Sysco mobile device configuration standards.

- The software will require that a secure password is used to access the device (8 characters, meeting Sysco complexity standards), and will authorize Sysco to erase all content on the device, should it be lost, stolen, or when you are no longer employed by Sysco.
- Your device will also be configured to automatically lock when not being used, and will be configured to be considered stolen, if 10 unsuccessful attempts are made to unlock the device. If considered stolen, all device contents will be erased.

  Warning: 10 unsuccessful attempts to access the device will result in the device contents being erased.
- It is against Sysco policy to attempt to override or bypass these configuration changes, and/or to bypass standard security features of the device that cannot be inherently changed through standard device menus.

3. Use of Cameras and Recording Devices

Do not make available to external parties any photos, videos, and/or audio recordings that contain internal Sysco information and/or assets, unless authorized by management.

- Drivers are required to use Sysco-issued cameras when capturing images and/or videos of vehicular incidents involving Sysco-branded vehicles. If no Sysco-issued camera is available, images can be captured with an alternate device. Share such images *only* with Sysco management.

- Using mobile devices to make audio and/or video recordings of Sysco business discussions is prohibited, unless an audible approval from each participant is recorded at the beginning of the recording; or written approval is received from each individual being recorded in advance of the session.

4. Applying Patches and Updates

Mobile devices must be kept up-to-date with the most recent patches and software.

- Sysco associates, contractors and partners are required to update their mobile devices within 30 days following the release of a new update.
- Mobile devices may be prevented from connecting to the Sysco network when Sysco no longer supports a device.
    - You will be notified in advance when Sysco will no longer support your device, and you will be required to update or upgrade your device in order to access the Sysco network.

5. Ensuring Security of Sysco Content

Sharing of internal Sysco information is restricted to those with a business need, and only approved methods must be used for sharing the information.

- Do not send internal Sysco information to or from your personal, non-Sysco email address.
- Do not post internal Sysco information from any device to public social networking, file sharing, or other publically available websites, unless Sysco management has explicitly authorized the publishing of this information.
- Do not use online storage apps and/or websites to store internal Sysco information, unless explicitly identified by Sysco as an approved storage location; or explicit approval has been received from management.
- Do not connect your device to insecure Wi-Fi networks (those that are configured to allow connection without a password, or configured to use "WEP") unless a VPN connection is opened immediately after connecting to the insecure network.

Note: This section does not restrict the right of an employee to engage in activities protected by law.

6. Internet Usage

The Sysco Information Security Policy governs the use of the internet on mobile devices, just as it does in the workplace.

Note: The definition of workplace extends beyond the confines of enterprise facilities. The workplace also includes meeting areas, conferences, vendor facilities, and any other location where exposure and display of content might reflect on the company.

7. Email Usage

All Sysco emails sent from a mobile device are required to meet all requirements outlined in the Sysco overarching Information Security Policy including the following:

- Use Sysco-issued email addresses for business purposes only.

- You represent Sysco, and email you send must comply with all local policies and with the Sysco Code of Conduct.

8. Applications and Downloads

By connecting a mobile device to the Sysco network, you are authorizing the installation of Sysco mobile device management software, or any other software deemed necessary by Sysco to ensure that your device remains in compliance with Sysco policies and standards.

- Downloading platform specific applications to your device is acceptable, as long as the application complies with this policy, the Sysco Information Security policy, the Sysco Code of Conduct, and is not restricted for use by Sysco.
- You will be responsible for ensuring that installed applications remain up-to-date.

Related Policies and Documents

Sysco has adopted standards, guidelines, procedures, tools, and training materials to help you properly manage Sysco information:

- Sysco Enterprise Security SharePoint Homepage
  - Sysco Information Security Policy
- Mobile Technologies SharePoint site
  - Sysco Corporate Approved Devices
- Sysco Human Resources SharePoint site
  - Sysco Code of Conduct Booklet
  - Sysco Corporate Associate Handbook
    Responsible Utilization of Communication Systems
  - Sysco Social Media Policy

Contact Information

For information about this policy or for general advice on information security, contact **Information Security** via email: 000-InfoSec@corp.sysco.com.

Contact the **Customer Support Group (CSG)** to initiate a full wipe of the contents on lost/stolen/compromised devices, and to receive mobile device setup instructions.

- phone: 281.584.1190
- email: 000-CUSTOMER.SUPPORT@corp.sysco.com

Additional Information

Reporting and Investigations

It is very important that you immediately report any known or suspected violations of this policy, contact your direct supervisor or another member of management, your Human Resources business partner, or call the AlertLine, a confidential toll-free, third party-operated telephone service.

You may also submit a report via the AlertLine website: https://syscoethics.alertline.com, a confidential web-based online reporting vehicle. Anyone reporting a suspected or actual violation of this policy in good faith is protected from retaliation under the Sysco Code of Conduct. All good faith allegations of violations of this policy will be fully and confidentially investigated. You are required to cooperate with all investigations of alleged policy violations.

Discipline and Other Consequences

Associates who violate this policy will be subject to appropriate disciplinary action or other remedial measures up to and including termination of employment, if warranted under the circumstances and permissible under applicable law. Assigned workers and third parties who violate this policy are subject to being denied access to Sysco facilities, personnel and assets, and permission to perform services on Sysco's behalf.

Waivers

No waiver of any provision of this policy shall be enforceable unless in writing and signed by the Policy Owner. No waiver of any provision of this policy in any one or more instances shall constitute a waiver in any other instance.

Revision and Revocation

This policy is not a contract between Sysco and any associate, assigned worker, or Third Party. This policy may be revised or revoked by the policy Owner at any time, without advance notice or cause.

Local Policies and Procedures

Sysco operates in many countries, states, provinces, and jurisdictions, and it is Sysco's intent to comply with all applicable legal requirements. Accordingly, if a provision of this policy conflicts with applicable local legal requirements, Sysco may adopt regional or country-specific policies on this subject to accommodate local conditions or comply with legal requirements. In such a case, you must comply with all applicable local policy and procedures. This policy will be applied in accordance with applicable local, state, and federal laws. Nothing in this policy shall be construed to restrict employee activities protected by law.

Appendix A

Roles and Responsibilities

Mobile Technologies maintains and publishes a list of approved mobile devices.

Enterprise Security issues and enforces the Mobile Device Policy.

Information Security is responsible for the following:

- Conducting regular risk assessments to determine if shifts in external threats or technology advances warrant revising the Mobile Device Policy
- Reviewing and updating the Mobile Device Policy annually
- Making Sysco associates and partners aware of security threats to mobile devices, and current policies governing the use of mobile devices

Policy Revisions

Change Record

Effective Date	Version	Published by	Summary of Change Approved by
6/11/13	1.0	Information Security	New policy published in SharePoint. Enterprise communication not sent at this time.
9/25/13	1.2	Information Security	Minor update with Mobile Technologies feedback. Released to enterprise, release email communication sent September 26.

Approval Matrix

Function	Name	Department
Technical Stakeholder(s)	Lauren Tran, Don Harrison	Mobile Technologies
HR	Ashley Michael	Human Resources
Legal	Eve McFadden, Tom Kurz	Legal
Policy Ownership	John Holzem, Curtis Simpson	Enterprise Security
Executive Policy Ownership	Wayne Shurts	Business Technology

Policy Location: http://mysysco/sites/security/default.aspx

FreshPoint Dallas Mobile Phone/Device Policy

Purpose:
FreshPoint Dallas, Inc. issues individual mobile phones/devices to associates whose jobs require them to be accessible for work-related matters. While mobile phones/devices are a necessary convenience of the business, we require that our Associates follow the guidelines listed below for their own and others safety.

Policy:
All Associates are required to be professional and conscientious at all times when using company phones. Your use of company-issued mobile phones/devices must comply with all company polices, including the Sysco Code of Conduct, policies prohibiting unlawful discrimination and harassment, and the policies outlined in this document.

Mobile phones/devices issued by the Company are Company property and are considered Company assets. Associates must comply with Company requests to make their Company-issued mobile phones/devices available for any reason, including upgrades, replacement, or inspection. Associates who leave the Company for any reason must return Company-issued mobile phones/devices without exception.

Personal Use of Company-Issued Mobile phones/devices:
It is FreshPoint Dallas, Inc. policy that Associates who are issued a mobile phone/device understand such items are issued for business use. Associates are expected to make every effort to not exceed the current contracted usage limits. Associates may be required to reimburse the Company for any costs or charges relating to personal use of their assigned mobile phones/devices for texting, voice calls and data usage, etc… Mobile phone/device bills are reviewed when received. Any Associate who exceeds their contracted usage limits is subject to additional usage review.

Security of Company-Issued Phones:
Associates are responsible for the security of Company-issued mobile phones/devices and the information stored on them. Always keep your mobile phone/device with you when traveling; never leave it unattended. Never store confidential Company information on a mobile phone/device. If your Company-issued mobile phone/device is lost or stolen, notify your immediate supervisor or your local Human Resources Department **immediately**. The cost to repair (*for other than normal wear and tear*) or replace lost or stolen mobile phones/devices will be charged to the associate to whom the phone/device was issued.

Be advised that this policy does not supersede the Electronic Device Usage or Social Media Policies.

FreshPoint Dallas, Inc. reserves the right to amend or alter the terms of this policy.

Associates found to be in violation of any part of this policy will be subject to disciplinary action, up to and including possible termination of employment.

Acknowledgment of Mobile Phone/Device Policy

I, _____, have received, read and understand the FreshPoint Dallas, Inc. Mobile Phone/Device Policy. I further understand that I am responsible for the cost to repair (*for other than normal wear and tear*) or replace a lost or stolen mobile phones/devices assigned to me. I also understand that if I leave the Company's employment, I am responsible for returning to the Company all mobile phones/devices assigned to me in working condition, and if I fail to do so, I authorize the Company to make a deduction from my final wages or any other Company compensation program for the replacement cost.

_____

Associate Name **Associate Signature** **Date**